UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/573,367	02/23/2007	Philippe Guillot	11345/077001	2146

22511 7590 05/06/2010

OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

EXAMINER	
TOLENTINO, RODERICK	
ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
05/06/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@oshaliang.com
buta@oshaliang.com

Office Action Summary	Application No.	Applicant(s)	
	10/573,367	GUILLOT ET AL.	
	Examiner	Art Unit	
	Roderick Tolentino	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 March 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/24/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 22 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

The Specification of the instant application describes that the present invention can be implemented as software, thereby rendering the "means for" language in claim(s) 16 and 22 as computer software. *In re Donaldson Co.*, 16 F.3d 1189, 29 USPQ2d 1845 (Fed. Cir. 1994), decided that

> the "broadest reasonable interpretation" that an examiner may give means-plus-function language is that statutorily mandated in paragraph six. Accordingly, the PTO may not disregard the structure disclosed in the specification corresponding to such language when rendering a patentability determination.

See MPEP § 2181 also. Therefore, giving the claims their broadest reasonable interpretation, while keeping the structure disclosed in the specification in my mind, one of ordinary skill

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1 – 7, 11 – 16 and 19 – 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Le Buhan et al. U.S. PG-Publication No. (2006/0107045).

5. As per claim 1, 15 and 22, Le Buhan discloses selecting a first key, the first key being unique in the broadcasting network, determining a second key according to the first key, such that a combination of the control data that is received to be decrypted by each receiving decoding system, the encrypted control data being identical for each receiving decoding system (Le Buhan, Paragraph 0047, asymmetric key pairs in a decoding system), assigning respectively the first key and the second key to the first element and the second element (Le Buhan, Paragraph 0047, asymmetric key pairs in a decoding system).

6. As per claim 2, Le Buhan discloses the control data enables to descramble the scrambled audiovisual information, the method further comprising: receiving at the first decoding system the encrypted control data; using the first key at the first element and using the second key at the second element to decrypt the encrypted control data (Le Buhan, Paragraph 0044, encrypting and decrypting data).

7. As per claim 3, Le Buhan discloses the control data is a control word, the audiovisual information being scrambled using the control word (Le Buhan, Paragraph 0015, control-words).

8. As per claim 4, Le Buhan discloses the control data is an Entitlement Control Message (ECM) comprising a control word, the audiovisual information being scrambled using the control word (Le Buhan, Paragraph 0047, ECM).

9. As per claim 5, Le Buhan discloses the control data is an exploitation key, the exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word (Le Buhan, Paragraph 0052, getting control word to decrypt data).

10. As per claim 6, Le Buhan discloses the control data is an Entitlement Management Message (EMM) comprising an exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word (Le Buhan, Paragraph 0021, Local control message).

11. As per claim 11, Le Buhan discloses the encrypted information is the scrambled audiovisual information (Le Buhan, Paragraph 0052, getting control word to decrypt data).

12. As per claim 12, Le Buhan discloses the encrypted information is a control word, the audiovisual information being scrambled using the control word (Le Buhan, Paragraph 0052, getting control word to decrypt data).

13. As per claim 13, Le Buhan discloses respectively attributing the first key and the second key at least to a third element and a fourth element forming a second decoding system distinct from the first decoding system (Le Buhan, Paragraph 0052, getting control word to decrypt data).

14. As per claim 14, Le Buhan discloses the first element is a decoder; the second element is a portable security module (Le Buhan, Paragraph 0010, portable device).

15. As per claim 16, Le Buhan discloses receiving means to receive the broadcasted encrypted control data; a pair of decryptions comprising a first decryption and a second decryption respectively located in the first element and the second element, the pair of decryptions enabling to decrypt the broadcasted encrypted control data using the first key and the second key (Le Buhan, Paragraph 0047, asymmetric key pairs in a decoding system).

16. As per claim 19, Le Buhan discloses the control data is a control word, the audiovisual information being scrambled using the control word (Le Buhan, Paragraph 0052, getting control word to decrypt data).

17. As per claim 20, Le Buhan discloses the control data is an exploitation key, the exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word (Le Buhan, Paragraph 0052, getting control word to decrypt data).

18. As per claim 21, Le Buhan discloses the first element is a decoder; the second element is a portable security module (Le Buhan, Paragraph 0010, portable device).

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

20. Claims 7 – 10, 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Le Buhan et al. U.S. PG-Publication No. (2006/0107045) in view of Kocher et al. U.S. PG-Publication No. (2001/0002486).

21. As per claim 7, Le Buhan fails to teach selecting a first prime number p and a second prime number q; calculating a modulus number n as being equal to a product of the first prime number p and the second prime number q; selecting an encrypting key e as being smaller to the modulus number and as being prime with a function of the first prime number p and the second prime number q; determine a private key as being equal to an inverse of the encrypting key modulus the function of the first prime number p and the second prime number q; selecting the first key and the second key such that a product of the first key and the second key equals the private key modulo the function of the first prime number p and the second prime number q; erasing the first prime number p and the second prime number q. However, in an analogous art Kocher teaches selecting a first prime number p and a second prime number q; calculating a modulus number n as being equal to a product of the first prime number p and the second prime number q; selecting an encrypting key e as being smaller to the modulus number and as being prime with a function of the first prime number p and the second prime number q; determine a private key as being equal to an inverse of the encrypting key modulus the function of the first prime number p and the second prime number q; selecting the first key and the second key such that a product of the first key and the second key equals the private key modulo the function of the first prime number p and the second

prime number q; erasing the first prime number p and the second prime number q (Kocher, Paragraph 0076, RSA).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Kocher's leak-resistant cryptographic method in view of Le Buhan's method for verifying validity of domestic digital network key because it offers the advantage of preventing attackers from accessing keys (Kocher, Paragraph 0003).

22. As per claim 8, Le Buhan as modified teaches receiving at each receiving decoding system a message comprising the encrypted control data; decrypting the encrypted control data using the first key at the first element and the second key at the second element (Le Buhan, Paragraph 0052, getting control word to decrypt data).

23. As per claim 9, Le Buhan as modified teaches the encrypted control data is decrypted using a discrete logarithms algorithm, the method further comprising: selecting a prime number q; selecting a primitive root of the prime number g; and wherein a product of the first key and the second key equals a private key modulo the prime number (Kocher, Paragraph 0076, RSA).

24. As per claim 10, Le Buhan as modified teaches receiving at each receiving decoding system a message comprising an encrypted information encrypted with a cession key, the message also comprising the primitive root of the prime number g power a random number k; using the first key at the first element and using the second key at the second element to calculate the cession key from the prime number power the random number k; decrypting the encrypted information using the cession key (Kocher, Paragraph 0076, RSA).

25. As per claim 17, Le Buhan fails to teach wherein the broadcasted encrypted control data is decrypted using a discrete logarithm algorithm. However, in an analogous art Kocher teaches the broadcasted encrypted control data is decrypted using a discrete logarithm algorithm (Kocher, Paragraph 0076, RSA).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Kocher's leak-resistant cryptographic method in view of Le Buhan's method for verifying validity of domestic digital network key because it offers the advantage of preventing attackers from accessing keys (Kocher, Paragraph 003).

26. As per claim 18, Le Buhan as modified teaches the broadcasted encrypted control data is decrypted using a RSA algorithm (Kocher, Paragraph 0076, RSA).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on Monday - Friday 9am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Roderick Tolentino
Examiner
Art Unit 2439

Roderick Tolentino
/R. T./
Examiner, Art Unit 2439

/Edan Orgad/
Supervisory Patent Examiner, Art Unit 2439